(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) Offenlegungsschrift

(10) DE 198 18 998 A 1

(51) Int. Cl.[6]:
H 04 L 9/32
G 06 K 19/073
// H04Q 7/32

(21) Aktenzeichen: 198 18 998.2
(22) Anmeldetag: 28. 4. 98
(43) Offenlegungstag: 4. 11. 99

DE 198 18 998 A 1

(71) Anmelder:
Giesecke & Devrient GmbH, 81677 München, DE

(72) Erfinder:
MacDonald, Donald, 80538 München, DE; Vedder, Klaus, Dr., 80801 München, DE; Richter, Oliver, 81827 München, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Verfahren zum Schutz vor Angriffen auf den Authentifizierungsalgorithmus bzw. den Geheimschlüssel einer Chipkarte

(57) Die Erfindung betrifft ein Verfahren zum Schutz vor Angriffen auf den Authentifizierungsalgorithmus bzw. den Geheimschlüssel einer Chipkarte (SIM) in einem Netzwerk zur Nachrichtenübertragung, vorzugsweise in einem GSM-Netzwerk, bei dem in einer Chipkarte (SIM) ein Algorithmus sowie ein geheimer Schlüssel gespeichert ist, wobei zur Authentifizierung zunächst vom Netzwerk oder einer Netzwerkkomponente eine Zufallszahl an die Chipkarte übertragen wird, in der Chipkarte mittels des Algorithmus, der Zufallszahl und des geheimen Schlüssels ein Antwortsignal erzeugt wird, das an das Netzwerk bzw. die Netzwerkkomponente übermittelt wird, um dort die Authentizität der Karte zu überprüfen. Gemäß der Erfindung ist ein Zähler zur Aufzeichnung der Anzahl der insgesamt mit der Karte durchgeführten Authentifikationsvorgänge vorgesehen. Es wird weiterhin ein oberer Grenzwert für die Anzahl der insgesamt mit der Karte durchzuführenden Authentifikationsvorgänge vorgegeben und bei jeder Authentifikation der Zähler erhöht und mit dem vorgegebenen oberen Grenzwert verglichen.

DE 198 18 998 A 1

Beschreibung

Die Erfindung betrifft ein Verfahren zum Schutz vor Angriffen auf den Authentifizierungsalgorithmus bzw. den Geheimschlüssel einer Chipkarte (SIM) in einem Netzwerk zur Nachrichtenübertragung, vorzugsweise in einem GSM-Netzwerk, nach dem Oberbegriff des Anspruchs 1.

Bei GSM-Systemen ist es bekannt, daß sich zum Gebrauch der Chipkarte (Subscriber Identity Module SIM) zunächst der Benutzer mittels einer persönlichen Identifikationsnummer (PIN) als zur Benutzung berechtigt ausweisen muß. Um an dieser Stelle Mißbrauch zu vermeiden, ist es für die PIN-Eingabe bekannt, einen Fehlerzähler vorzusehen, der nach Überschreiten einer zulässigen Anzahl von Fehlversuchen den weiteren Gebrauch der Karte unterbindet.

Eine weitere, systemrelevante Sicherheitsmaßnahme besteht in der Authentisierung der Karte gegenüber dem Mobilfunknetz. Zu diesem Zweck ist in der Karte eine von außen nicht zugängliche Geheimnummer und ein ebenfalls von außen nicht zugänglicher, gegebenenfalls geheimer Algorithmus abgelegt. Zur Authentifizierung wird vom Netzwerk bzw. einer Netzwerkkomponente eine Zufallszahl erzeugt, die der Karte mitgeteilt wird. Die Karte berechnet aus dieser Zufallszahl und dem geheimen Schlüssel mittels des Algorithmus eine Signalantwort, welche dem Netzwerk mitgeteilt wird. Diese Antwort wird im Netzwerk analysiert und es wird, bei positivem Ergebnis, Zugang zu den Netzwerkfunktionen erlaubt.

Aus der deutschen Patentschrift DE 43 39 460 C1 ist ein Verfahren zur Authentifizierung eines Systemteils durch ein anderes Systemteil eines Informationsübertragungssystems nach dem Challenge and Response-Prinzip bekannt. Die dort beschriebene Datenträgeranordnung ist mit einem Wertespeicher versehen, dem eine Kontrolleinrichtung zugeordnet ist. Weiterhin ist ein nicht flüchtiger, begrenzbarer Fehlerzähler sowie eine Sperrvorrichtung vorgesehen. Bei dem Authentifizierungsverfahren ist die tragbare Datenträgeranordnung zunächst gesperrt und wird erst nach Verändern des Fehlerzählerstandes freigegeben. Von dem Endgerät werden daraufhin Zufallsdaten zur tragbaren Datenträgeranordnung übertragen. Diese Daten werden sowohl im Endgerät als auch in der tragbaren Datenträgeranordnung durch einen geheimen Algorithmus und geheime Schlüsseldaten zu Authentifikationsparametern verarbeitet. Die im Endgerät erzeugten Authentifikationsparameter werden im weiteren zur tragbaren Datenträgeranordnung übermittelt und mit den dort berechneten Authentifikationsparametern verglichen. Bei Übereinstimmung wird der Fehlerzähler rückgesetzt.

Bei dem bekannten Stand der Technik wird also bei jedem Bearbeitungsvorgang der Fehlerzähler erhöht und bei erfolgreicher Beendigung des Bearbeitungsverfahrens rückgesetzt. Bei Überschreiten eines vorgegebenen Grenzwertes für die Anzahl der Fehlversuche werden weitere Authentifizierungsversuche nicht zugelassen.

Bei der Authentifizierung im GSM-Netz besteht das Problem, daß die Karte nicht über eine fehlgeschlagene Authentifizierung informiert wird, sondern es wird lediglich im System eine Überprüfung durchgeführt, die entweder zum Abbruch der Verbindung oder zur Zulassung des Teilnehmers zu den Netzdiensten führt.

Auch in einem derartigen Netz besteht die Gefahr, daß durch Angriffe auf den Algorithmus, der zur Authentifizierung verwendet wird, das Netzwerk beispielsweise in einem Computer simuliert werden kann, indem ausgewählte "Zufallszahlen" nach dem standardisierten Protokoll an die SIM-Karte übermittelt werden und daraus bei mehrfachen Authentifizierungsversuchen der Geheimschlüssel der Chipkarte ermittelt werden kann. Nach Ermittlung des geheimen Schlüssels und bei Bekanntsein des Algorithmus können wesentliche Funktionselemente der Karte simuliert bzw. dupliziert werden.

Es ist deshalb Aufgabe der Erfindung, ein sicheres Verfahren zum Schutz vor Angriffen auf den Authentifizierungsalgorithmus bzw. den Geheimschlüssel einer Chipkarte in einem Nachrichtensystem anzugeben, bei dem eine sichere Rückmeldung über die Authentifizierung an die teilnehmende Chipkarte nicht erfolgt.

Diese Aufgabe wird gemäß der Erfindung ausgehend von den Merkmalen des Oberbegriffs des Anspruchs 1 durch die kennzeichnenden Merkmale des Anspruchs 1 gelöst.

Vorteilhafte Ausgestaltungen der Erfindung sind in den abhängigen Ansprüchen angegeben.

Gemäß der Erfindung wird vorgeschlagen, die beliebig häufige Wiederholung des Identifizierungsvorgangs dadurch zu unterbinden, daß in der Karte oder im Netzwerk ein Zähler vorgesehen wird, welcher die Anzahl der insgesamt durchgeführten Authentifizierungsversuche festhält. Der aktuelle Zählerstand wird bei jeder Authentifizierung mit einem vorgebbaren oberen Grenzwert verglichen. Durch die Zählung der Anzahl der insgesamt durchgeführten Authentifikationsversuche wird in vorteilhafter Weise zum einen erreicht, daß die fehlende Rückmeldung des Authentifizierungsergebnisses nicht zwangsläufig in der Nichtanwendbarkeit der Vorgabe einer Obergrenze für die maximal zulässige Anzahl der Authentifizierungsversuche endet und zum anderen kann der Zähler, da ein Rücksetzen nicht erlaubt ist, durch ein unzulässiges Rücksetzsignal nicht außer Kraft gesetzt werden.

Gemäß einer vorteilhaften Ausführungsform der Erfindung liegt der vorgegebene obere Grenzwert höher als die geschätzte Anzahl der mit der Karte üblicherweise auszuführenden Authentifikationsvorgänge. Zur Auslegung der oberen Grenze ist deshalb jeweils an Hand der Schlüssellänge und der sonstigen Randbedingungen eine Risikoabschätzung durchzuführen, wobei bei vertretbarem Risiko die obere Grenze möglichst über der Anzahl der zu erwartenden regulären Authentifikationen anzusetzen ist, um nicht eine für den Benutzer unangenehme vorzeitige Sperrung der Karte in Kauf zu nehmen. Die vorgegebene obere Grenze sollte überdies unter der zu erwartenden Anzahl der Versuche liegen, die notwendig sind, um den geheimen Schlüssel herauszufinden.

Eine weitere vorteilhafte Ausgestaltung der Erfindung sieht vor, daß der Zähler in der Chipkarte realisiert ist und der Vergleich mit dem oberen Grenzwert in der Chipkarte ausgeführt wird. Damit kann bei einer Simulation des Netzes durch einen Computer zumindest die Simulation der Zählerstände vermieden werden.

Für den Fall, daß beispielsweise aufgrund mangelnden Speicherplatzes oder sonstiger Umstände eine Realisierung des Zählers auf der Karte nicht möglich ist, kann die Realisierung auch im Netz erfolgen, wobei vorzugsweise die Zählerdaten vor jeder Authentifizierung verschlüsselt an die Karte übertragen werden.

Gemäß einer weiteren vorteilhaften Ausgestaltung der Erfindung werden bei Überschreiten des oberen Grenzwertes einzelne oder alle Funktionen der Chipkarte blockiert, so daß die Funktionsfähigkeit der Karte zumindest stark eingeschränkt wird.

Alternativ oder zusätzlich kann bei Überschreiten des Grenzwertes an das Netzwerk oder eine entsprechende Netzwerkkomponente eine Information übermittelt werden, wodurch im Netzwerk die Funktionen der Karte (SIM) zumindest überwacht werden können. Mit dieser Information können ferner seitens des Netzwerkes bzw. der Netzwerkkomponente einzelne oder alle Funktionen der Karte ge-

sperrt werden.

Es ist ferner vorteilhaft, in allen ATR-Berichten der Karte auf das Überschreiten der oberen Grenze hinzuweisen.

Insbesondere für den Fall, daß die obere Grenze für die zulässige Anzahl an Authentifizierungsverfahren mit hoher Wahrscheinlichkeit kleiner als die zu erwartende reguläre Anzahl von Authentifizierungen ist, ist es vorteilhaft, einen alternativen geheimen Schlüssel in der Karte abzulegen. Bei Erreichen der oberen Grenze kann somit auf einen neuen Geheimschlüssel umgestellt werden, wobei hierbei ebenfalls ein neuer Zähler initiiert wird bzw. der Zähler rückgesetzt wird.

Neben dem Umschalten auf einen weiteren geheimen Schlüssel, kann ebenfalls eine neue IMSI selektiert werden, so daß nach Erreichen des oberen Grenzwertes auf ein neues IMSI/Schlüssel-Paar zugegriffen wird.

Insbesondere für SIM's, die über eine eigene Energieversorgung und damit über eine interne Zeitmessung verfügen können, kann es auch vorteilhaft sein, nach einer längeren Zeitdauer den Zähler zyklisch rückzusetzen.

Es kann weiterhin neben dem oberen Grenzwert ein zweiter Grenzwert vorgesehen werden, der unter dem oberen Grenzwert liegt. Damit ist die Möglichkeit gegeben, dem Netzwerk bereits vor Erreichen des oberen Grenzwertes eine Information zukommen zu lassen, die es dem Netzwerkbetreiber erlaubt, beispielsweise dem Benutzer rechtzeitig eine neue Karte auszustellen, wenn die Funktionen der im Gebrauch befindlichen aufgrund der Überschreitung der zulässigen Anzahl an Authentifikationen in absehbarer Zeit gesperrt werden.

Im folgenden wird die Erfindung beispielhaft anhand eines Ausführungsbeispiels gemäß den **Fig.** 1 und 2 beschrieben.

Fig. 1 zeigt den Ablauf der kryptographischen Funktionen des SIM im GSM-Netz.

Fig. 2 zeigt die für die Erfindung wesentlichen Elemente des SIM.

In **Fig.** 1 ist der Datenaustausch zwischen der Chipkarte (SIM) und dem Netzwerk über die Luftschnittstelle dargestellt.

Bei der **Fig.** 1 wird vorausgesetzt, daß der übliche Vorgang der PIN-Verifizierung abgeschlossen ist. Im Anschluß an diese PIN-Verifizierung wird von mobilen Einheit, in der sich die Karte befindet, eine Nachricht an das Netzwerk gesendet, welche die IMSI (international mobile subscriber identity) bzw. TMSI (temporary mobile subscriber identity) enthält. Aus der IMSI bzw. TMSI wird im Netzwerk nach einer vorgegebenen Funktion oder mittels einer Tabelle der geheime Schlüssel K_i ermittelt, der in der Chipkarte (SIM) in einem nicht zugänglichen Speicherbereich abgelegt ist. Der geheime Schlüssel wird für die spätere Verifizierung des Authentifikationsvorganges benötigt.

Vom Netzwerk wird der Authentifizierungsvorgang initialisiert, indem eine Zufallszahl (RAND) berechnet wird, die über die Luftschnittstelle in die Chipkarte (SIM) übertragen wird.

In der Chipkarte wird daraufhin mittels einer Authentisierungsfunktion aus dem geheimen Schlüssel K_i und der Zufallszahl RAND das Authentisierungsergebnis SRES gebildet, das über die Luftschnittstelle an das Netzwerk übertragen wird. Im Netzwerk wird ebenfalls mittels der geheimen Funktion und der Zufallszahl RAND sowie dem geheimen Schlüssel K_i ein Authentisierungsergebnis SRES' gebildet. Im Netzwerk findet weiterhin ein Vergleich der Authentisierungsergebnisse SRES und SRES' statt, wobei bei Gleichheit der Authentifizierungsvorgang erfolgreich abgeschlossen wird, während bei Ungleichheit ein Abbruch der Verbindung vorgenommen wird, da sich die Karte des Teilnehmers nicht authentisiert hat.

In der Chipkarte SIM wird gemäß der Erfindung entweder vor oder nach der Authentisierung der Zählerstand eines Authentifikations-Zählers erhöht. Im Anschluß an die Zählererhöhung wird in der Chipkarte SIM ein Vergleich des aktuellen Zählerstandes mit dem oberen Grenzwert Z_{max}, welcher die maximal zulässige Anzahl der Authentifizierungsvorgänge angibt, verglichen. Für den Fall, daß $Z < Z_{max}$ ist, können im Netzwerk alle Dienste in Anspruch genommen werden, für die der Benutzer autorisiert ist. Für den Fall, daß der aktuelle Zählerstand Z den oberen Grenzwert Z_{max} erreicht oder überschritten hat, kann entweder chipkartenseitig eine Sperrung SP der Chipkarte und damit der Netzwerkfunktionen eingeleitet werden oder es kann alternativ oder zusätzlich eine Nachricht Mess an das Netzwerk übermittelt werden, woraufhin im Netzwerk verschiedene Aktionen eingeleitet werden können, wie beispielsweise die Überwachung der SIM-Aktivitäten, das Nichtzulassen bestimmter Dienste im Netzwerk, oder die Sperrung der gesamten Dienste, die der Benutzer üblicherweise nach erfolgreicher Authentifizierung in Anspruch nehmen kann.

Die **Fig.** 2 zeigt ein Ausführungsbeispiel einer Chipkarte SIM, die eine Schnittstelle S zum Datenaustausch mit einem Mobilfunktelefon aufweist sowie einen Mikroprozessor µp, der mit einem Zähler Z und einem Speicher M, M_g verbunden ist. Der Zähler Z kann im wesentlichen als Hardwarezähler ausgebildet sein oder er ist als Softwarezähler programmiert. Der Speicher ist unterteilt in den üblichen Speicherbereich M, in dem Daten ausgelesen und eingeschrieben werden können und in den geheimen Speicherbereich M_g, in dem zumindest der geheime Schlüssel K_i sowie der Authentisierungsalgorithmus abgelegt sind. Wenn über die Schnittstelle S die Zufallszahl RAND erhalten wird, initiiert der Mikroprozessor µP zum einen die Erhöhung des Zählers Z sowie den Vergleich des aktuellen Zählerstands mit der oberen Grenze Z_{max} und zum anderen wird aus dem geheimen Speicherbereich M_g der geheime Schlüssel K_i sowie der Algorithmus geladen, um die Authentifizierungs-Berechnung durchzuführen und das Ergebnis SRES zu erhalten.

Patentansprüche

1. Verfahren zum Schutz vor Angriffen auf den Authentifizierungsalgorithmus bzw. den Geheimschlüssel (K_i) einer Chipkarte (SIM) in einem Netzwerk zur Nachrichtenübertragung, vorzugsweise in einem GSM-Netzwerk, bei dem in einer Chipkarte (SIM) ein Algorithmus sowie ein geheimer Schlüssel (K_i) gespeichert ist, wobei zur Authentifizierung
   - zunächst vom Netzwerk oder einer Netzwerkkomponente eine Zufallszahl (RAND) an die Chipkarte übertragen wird,
   - in der Chipkarte mittels des Algorithmus, der Zufallszahl (RAND) und des geheimen Schlüssels (K_i) ein Antwortsignal (SRES) erzeugt wird, das an das Netzwerk bzw. die Netzwerkkomponente übermittelt wird, um dort die Authentizität der Karte (SIM) zu überprüfen,

   dadurch gekennzeichnet, daß
   - ein Zähler (Z) zur Aufzeichnung der Anzahl der insgesamt mit der Karte durchgeführten Authentifikationsvorgänge vorgesehen ist,
   - ein oberer Grenzwert (Z_{max}) für die Anzahl der insgesamt mit der Karte durchzuführenden Authentifikationsvorgänge vorgegeben wird, und
   - bei jeder Authentifikation der Zähler (Z) erhöht und mit dem vorgegebenen oberen Grenzwert (Z_{max}) verglichen wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß der obere Grenzwert (Z_{max}) höher liegt als die geschätzte, mit einer Karte durchgeführte Anzahl an Authentifikationen und niedriger liegt als die zu erwartende Anzahl der für die Ermittlung des geheimen Schlüssels notwendigen Authentifizierungsvorgänge.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß der Zähler (Z) in der Chipkarte implementiert ist und der Vergleich des aktuellen Zählerstandes mit dem oberen Grenzwert (Z_{max}) in der Chipkarte durchgeführt wird.

4. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß der Zähler in einer Netzwerkkomponente implementiert ist und der Vergleich des aktuellen Zählerstandes mit dem oberen Grenzwert (Z_{max}) in einer Netzwerkkomponente durchgeführt wird.

5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß bei Überschreiten des oberen Grenzwertes (Z_{max}) einzelne oder alle Funktionen der Chipkarte (SIM) blockiert werden.

6. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß bei Überschreiten des vorgegebenen oberen Grenzwertes (Z_{max}) an das Netzwerk oder eine Netzwerkkomponente eine Information übermittelt wird und das Netzwerk infolge dieser Information die Aktivitäten der Chipkarte (SIM) überwacht.

7. Verfahren nach Anspruch 6, dadurch gekennzeichnet, daß das Netzwerk eine Anfrage initiiert, gemäß der die Funktionen der Chipkarte gelöscht oder eingeschränkt werden.

8. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß nach Erreichen des oberen Grenzwertes (Z_{max}) in allen Answer to Reset-(ATR-)Berichten ein Hinweis erzeugt wird, daß der Zähler seinen Höchststand erreicht hat.

9. Verfahren nach einem der vorhergehenden Ansprüche 1 bis 8, dadurch gekennzeichnet, daß bei Erreichen des oberen Grenzwertes (Z_{max}) des Zählers das Netzwerk oder die Chipkarte (SIM) das Umschalten auf einen alternativen, in der Chipkarte abgelegten, Geheimschlüssel (K_i) initiiert.

10. Verfahren nach einem oder mehreren der Ansprüche 1 bis 9, dadurch gekennzeichnet, daß nach Erreichen des Höchststandes des Zählers (Z) auf ein alternatives IMSI/geheimes Schlüssel-Paar umgestellt wird.

11. Verfahren nach einem der Ansprüche 1 bis 10, dadurch gekennzeichnet, daß der Authentifikations-Zähler nach einer vorgegebenen Zeit zurückgesetzt wird.

12. Verfahren nach einem der Ansprüche 1 bis 11, dadurch gekennzeichnet, daß neben dem oberen Grenzwert (Z_{max}) ein zweiter Grenzwert vorgegeben wird, der unterhalb des oberen Grenzwertes liegt, und bei dessen Erreichen ein Signal an das Netzwerk gesendet wird, in dem auf das nahende Erreichen des oberen Grenzwertes (Z_{max}) hingewiesen wird.

Hierzu 1 Seite(n) Zeichnungen

- Leerseite -

Nummer: DE 198 18 998 A1
Int. Cl.[6]: H 04 L 9/32
Offenlegungstag: 4. November 1999

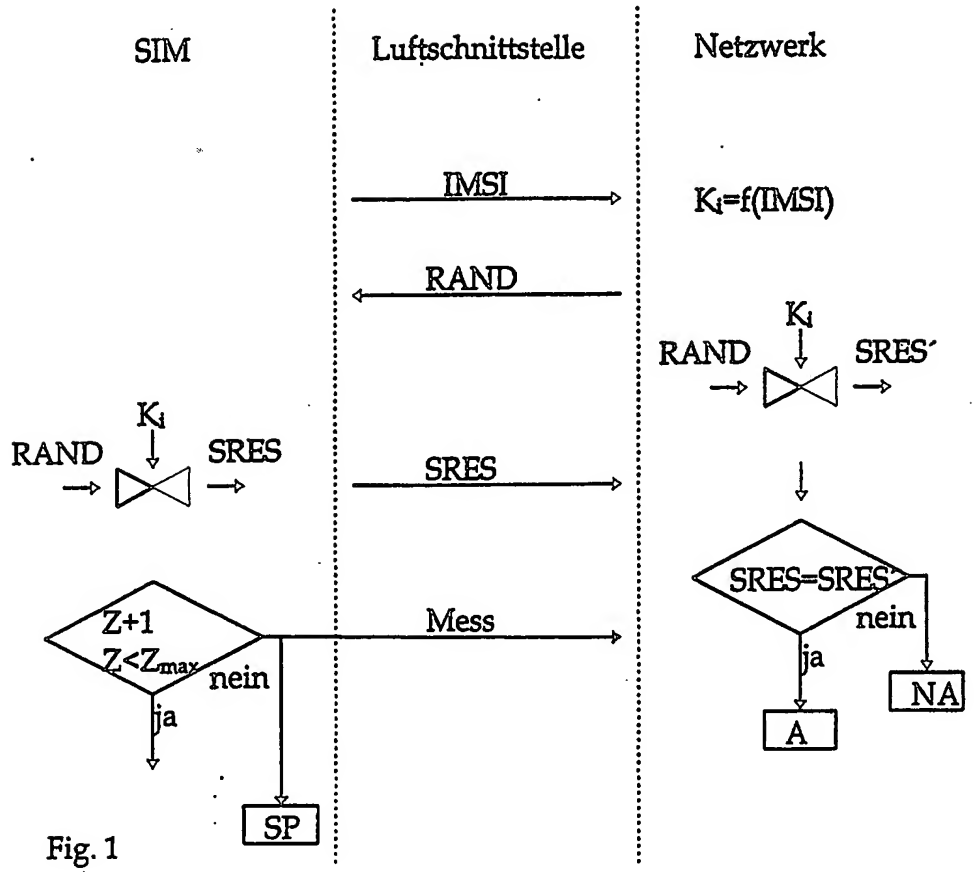

Fig. 1

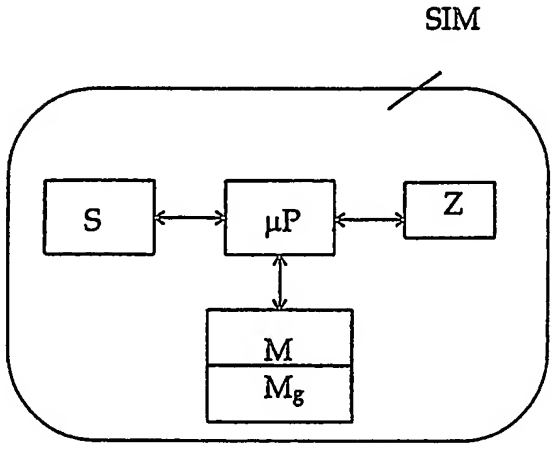

Fig. 2

DOCKET NO: 1999P2671
SERIAL NO:
APPLICANT: Brüdelmeier et al.

LERNER AND GREENBERG P.A.
P.O. BOX 2480
HOLLYWOOD, FLORIDA 33022
TEL. (954) 925-1100